IN THE CLAIMS

Please amend the claims as follows:

1-49. (Cancelled)

50. (Currently Amended) A device for providing a user with a secure access to a network resource, comprising:

a memory storing data related to at least one of accounts and preferences; and

a processor coupled to the memory, the processor authenticating the user with the device by verifying a device password and a user biometric that are specific to the device and transmitting a resource password to establish a connection to the network resource, the resource password being unknown to the user and specific to the network resource, wherein if a duress password is entered for authenticating the user, ~~the verification, the duress password being predetermined to be used when an access to the device is intended to be denied, and wherein the entry of the duress password~~ the processor replaces the data of the memory with non-sensitive data.

51. (Previously Presented) The device of claim 50, wherein the user is granted access to the memory upon verification.

52. (Cancelled)

53. (Cancelled)

54. (Previously Presented) The device of claim 50, wherein the data of the memory is encrypted, the data being decrypted with a device dependent key specific to the device.

55. (Previously Presented) The device of claim 50, wherein the user biometric is at least one of a path and a speed of a use of an input device, a fingerprint description, an iris scan, and a voice print.

56. (Previously Presented) The device of claim 55, wherein the path and the speed of the use of the input device include a signature of the device password to combine the device password and the biometric for the verification.

57. (Previously Presented) The device of claim 50, further comprising:

a true random number generator generating the resource password.

58. (Previously Presented) The device of claim 50, wherein the resource password is generated at a predetermined time for the access to the network resource.

59. (Previously Presented) The device of claim 50, wherein communications with the network resource are encrypted.

60. (Currently Amended) A method for authenticating a user to a device for contacting a network resource, comprising:

verifying a device password and a user biometric that are specific to the device;

transmitting a resource password to establish a connection to the network resource, the resource password being unknown to the user, the resource password being specific to the network resource;

receiving ~~entering~~ a duress password for authenticating the user ~~the verifying, the duress password being predetermined to be used when an access to the device is intended to be denied~~; and

replacing data of the memory with non-sensitive data when the duress password is received ~~entered~~.

61. (Previously Presented) The method of claim 60, further comprising:

upon the verifying, accessing a memory including at least one of accounts and preferences.

62. (Canceled)

63. (Cancelled)

64. (Previously Presented) The method of claim 61, wherein the data of the memory is encrypted, the data being decrypted with a device dependent key specific to the device.

65. (Previously Presented) The method of claim 60, wherein the user biometric is at least one of a path and a speed of a use of an input device, a fingerprint description, an iris scan, and a voice print.

66. (Previously Presented) The method of claim 65, wherein the path and the speed of the use of the input device include a signature of the device password to combine the device password and the biometric for the verifying.

67. (Previously Presented) The method of claim 60, further comprising:

generating the resource password using a true random number generator.

68. (Previously Presented) The method of claim 60, further comprising:

generating the resource password at a predetermined time for the access to the network resource.

69. (Previously Presented) The method of claim 60, wherein communications with the network resource are encrypted.

70. (Currently Amended) A device for providing a user with a secure access to a network resource, comprising:

a storage means for storing data related to at least one of accounts and preferences; and

a processing means for authenticating the user with the device by verifying a device password and a user biometric that are specific to the device and for transmitting a resource password to establish a connection to the network resource, the resource

password being unknown to the user and specific to the network resource, the processing means being coupled to the storage means, wherein if a duress password is entered for authenticating the user, ~~the verification, the duress password being predetermined to be used when an access to the device is intended to be denied, and wherein the entry of the duress password~~ the processing means replaces the data of the storage means with non-sensitive data.